Data Breach Response Planning: Laying the Right Foundation

September 16, 2015

Presented by

Paige M. Boshell

and

Amy S. Leopard

Bradley Arant Boult Cummings LLP

Attorneys from our Privacy and Information Security Team

Paige M. Boshell

- Co-Team Leader, Privacy & Information Security Team
- Partner, Birmingham Office

Amy S. Leopard

- Co-Team Leader, Privacy & Information Security Team
- Chair, AHLA Health Information and Technology Practice Group
- Vice Chair, HIMSS Legal Task Force
- Partner, Nashville Office

babc

Agenda

- Cybersecurity Planning
- Data Breach Plan (incident response)
- Cybersecurity Program
- FTC Enforcement of "Unfair" Security Practices
- FFIEC Cybersecurity Assessment Tool (financial institutions)
- Healthcare Enforcement
- HIPAA Security Breach Risk Assessment

babc

Cybersecurity Planning

- **National Institute of Standards and Technology ("NIST") Cybersecurity Framework**
  - Defined rubric and methodology for evaluating and addressing risk
  - Technology – neutral
  - Relies on existing requirements, best practices and industry standards
  - "Voluntary" for certain government contractors
  - Widespread impact – downstream chain, court and regulatory interpretations of reasonable or industry standard security practices and programs, applicability to variety of businesses

babc

Cybersecurity Planning

- Information Sharing and Analysis Centers (ISAC):
  - ISACs are trusted entities established by Critical Infrastructure Key Resource (CI/KR) owners and operators to provide comprehensive sector analysis, which is shared within the sector, with other sectors, and with government.
  - Services provided by ISACs include risk mitigation, incident response, alert and information sharing. The goal is to provide users with accurate, actionable, and relevant information.
  - Member benefits vary across the ISACs and can include: access to a 24/7 security operations center; briefings; white papers; threat calls; webinars; and anonymous CIKR Owner/Operator reporting.

babc

Cybersecurity Planning

- FS-ISAC: industry forum for collaboration on critical security threats facing the global financial services sector
  - Global cyber and physical threat intelligence analysis and sharing (anonymous information sharing)
  - Early warning of attacks
  - Collaboration in response
  - Coordination of assessment
- NH – ISAC: healthcare and public health critical infrastructure resilience
- Expert guidance on avoiding and mitigating attacks

babc

U.S. DOJ: Cyber Incident Best Practices
(April 2015)

Before Cyber Attack

- ID mission critical data and assets: "Crown Jewels"
- Actionable Incident Response Plan *before* intrusion,
  - Test and update contingency plans
- Align organizational policies (e.g. HR) with Incident Response Plan
- Obtain authorization, technology and services to permit lawful network monitoring and address incidents
- Ensure legal counsel is familiar with technology and cyber incident management to reduce incident response time
- Engage with law enforcement, outside counsel, PR Firms, cybersecurity firms
- Establish relationships with cyber information sharing organizations for best practices (ISACs)

babc

During A Cyber Attack

- Make initial assessment of scope and nature of incident
- Implement measures to minimize continuing damage
- Record and preserve data related to incident (image network, audit logs, records of attacks)
- Notify management, law enforcement, victims, DHS
  - HIPAA = > Individuals, HHS/OCR, Media,

DO NOT: use compromised systems to communicate OR
Hack back

After Recovering

- Continue monitoring for anomalous activity to document intruder expelled
  Who controls your network?
- Conduct Post-Incident review for deficiencies in Incident Response Plan
- Update and revise security policies or controls

"Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of ePHI." HIPAA 164.316(b)(2)(iii)

Cyber Incident Best Practices (US DOJ: April 2015)

FTC enforcement authority – Wyndham

2015 WL 4998121 (3d Cir. 8.24.15)

Section 5 of the FTC Act: "Unfair and Deceptive" Acts or Practices

Deceptive:

- Not implementing stated privacy policies
- Misrepresenting extent to which privacy and security of information collected, used, maintained is protected

Unfair:

- Alleged failure to implement reasonable and appropriate security measures
- Elements:
  - Practice causes or is likely to cause substantial injury to consumers
  - Consumers are not reasonably able to avoid injury
  - Injury is not outweighed by countervailing consumer benefit, competition

- Fair notice: That a company's conduct could fall within statute, not FTC's interpretation of cybersecurity practices.
  - FTC has published data security guidance and data security complaints

- MUST keep abreast of FTC guidance and complaints

babc

What is Fair Notice under *Wyndham*?

Issue	Card Systems Solutions (FTC 2006)[1]	Wyndham
Risk Assessment and Network Monitoring	Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks; did not implement simple, low-cost and readily available defenses to such attacks, CSS at ¶ 6(2)-(3).	Failed to monitor network for the malware used in a previous intrusion, Compl. at ¶ 24(i), reused by hackers later to access the system again, id. at ¶ 34.
Security Monitoring and Management Generally	Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations, CSS at ¶ 6(6).	Failed to employ reasonable measures to detect and prevent unauthorized access to computer network or to conduct security investigations, Compl. at ¶ 24(h).
Password Management	Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).	Did not employ common methods to require user IDs and passwords difficult for hackers to guess. (e.g., allowed remote access to a hotel's property management system that used default/factory setting passwords) Compl. at ¶ 24(f).
Maintenance of PI	Created unnecessary risks to personal information by storing it in a vulnerable format for up to 30 days, CSS at ¶ 6(1).	Allowed software to store payment card information in clear readable text, Compl. At ¶ 24(b).
Network Risk Management	Did not use readily available security measures to limit access between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).	Did not use readily available security measures, such as firewalls, to limit access between and among hotels' property management systems, the Wyndham network, and the Internet, Compl. at ¶ 24(a).

[1] No. C-4168 (FTC 2006)

10 FTC Lessons Learned from >50 Enforcement Actions

1. ***Start*** with Security.
2. Control ***access*** to data sensibly.
3. Require secure ***passwords*** and authentication.
4. ***Store*** sensitive personal information securely and protect it during ***transmission***.
5. Segment your ***network*** and monitor who's trying to get in and out.
6. Secure ***remote access*** to your network.
7. ***Control access*** to data sensibly.
8. Make sure your ***service providers*** implement reasonable security measures.
9. Put procedures in place to keep your security current and ***address vulnerabilities*** that may arise.
10. Secure ***paper, physical media, and devices***.

Source: FTC Lessons Learned from FTC Enforcement Actions business.ftc.gov

FFIEC Cybersecurity Assessment Tool

- FFIEC Cybersecurity Assessment Tool: intended to help financial institutions evaluate their own ISP and risk profile
  - Inherent Risk Profile
  - Cybersecurity Maturity

babc

FFIEC Cybersecurity Assessment Tool: Inherent Risk Profile

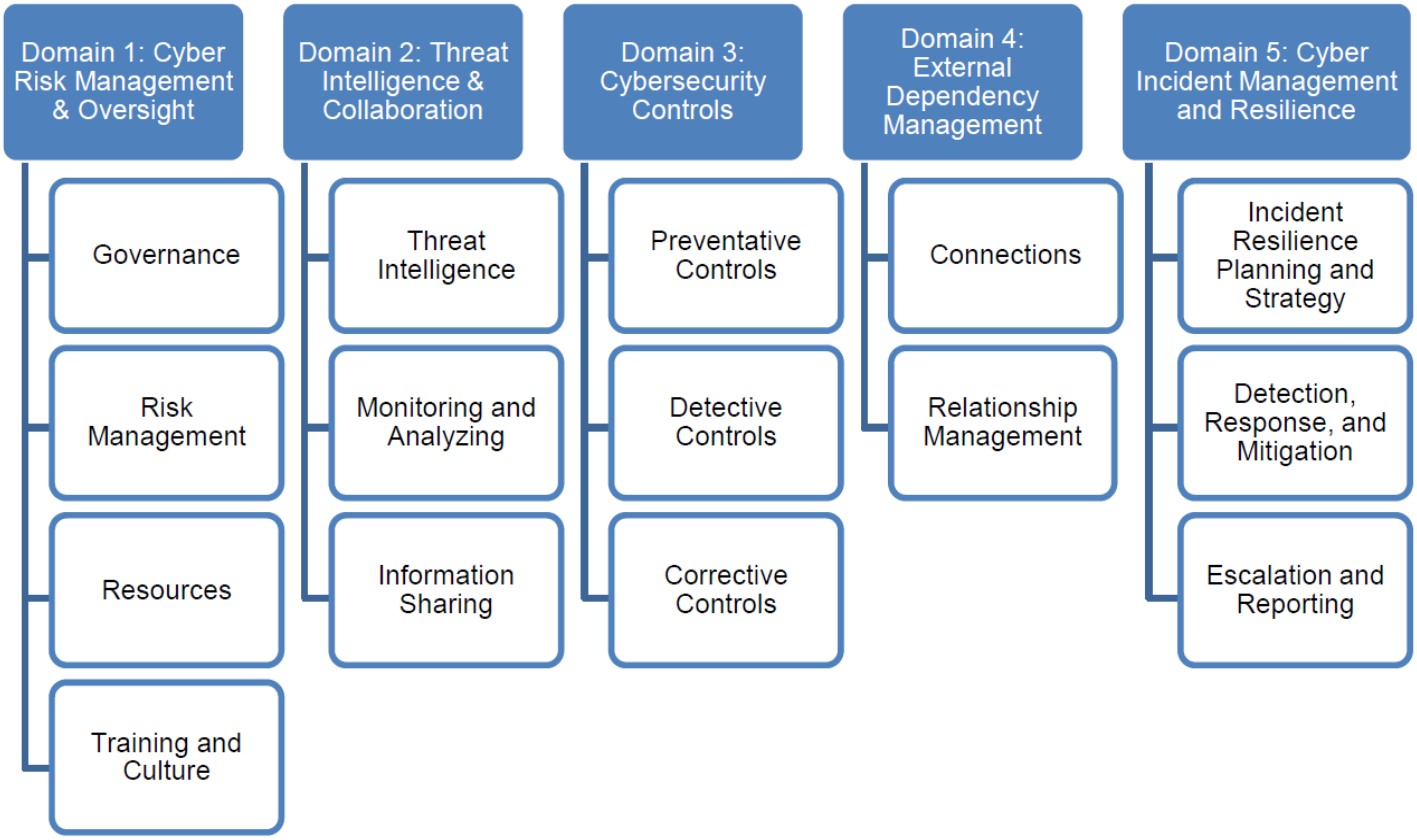
- Inherent Risk Profile - level of risk posed by the following:
  - Technologies and Connection Types
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organizational Characteristics
  - External Threats

FFIEC Cybersecurity Assessment Tool: Inherent Risk Profile

- Risk Levels – For each of the categories above, there is a risk level that the institution can choose based on descriptions provided in the Tool. For instance, in reviewing External Threats, institutions are given five risk levels to choose from, which are defined for each category. The table below illustrates the various risk levels.

Category: External Threats	Risk Levels				
	Least	Minimal	Moderate	Significant	Most
Attempted cyber attacks	No attempted attacks or reconnaissance.	Few attempts monthly (<100); may have had generic phishing campaigns by employees and customers.	Several attempts monthly (101-500); phishing campaigns targeting employees or customers at the institution or third parties supporting critical activities; may have experienced an attempted Distributed Denial of Service (DDoS) attack within the last year.	Significant number of attempts monthly (501-100,000); spear phishing campaigns targeting high net worth customers and employees at the institution or third parties supporting critical activities; Institution specifically is named in threat reports; may have experienced multiple DDoS attacks within the last year.	Substantial number of attempts monthly (> 100,000); persistent attempts to attack senior management and/or network administrators; frequently targeted for DDoS attacks.

FFIEC Cybersecurity Assessment Tool: Cybersecurity Maturity



babc

Bradley Arant Boult Cummings LLP

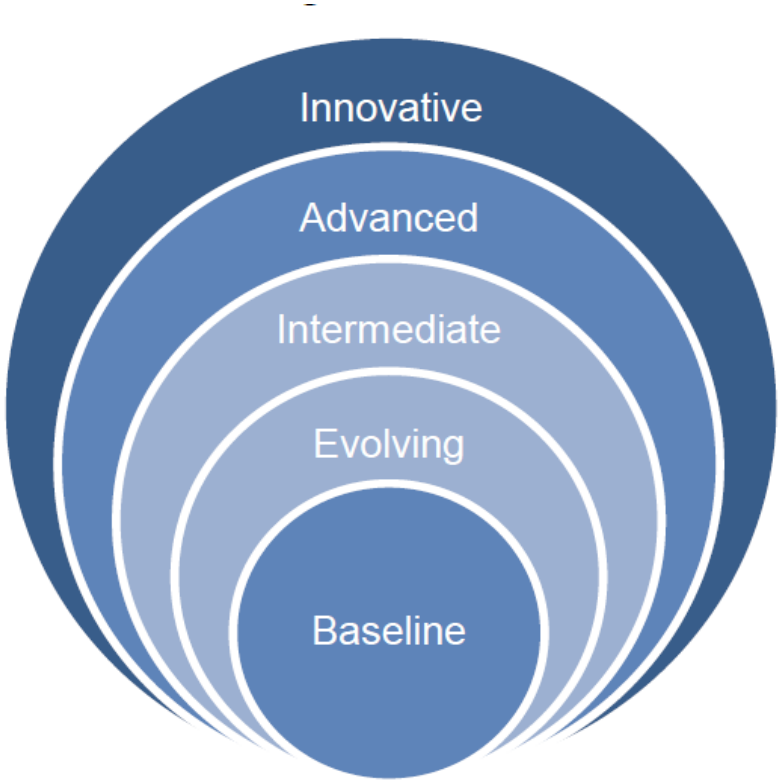
FFIEC Cybersecurity Assessment Tool: Cybersecurity Maturity

Domain 1: Cyber Risk Management and Oversight →Training and Culture → Culture

CULTURE	**Baseline**	Management holds employees accountable for complying with the information security program. *(FFIEC Information Security Booklet, page 7)*
	Evolving	The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures. Cyber risks are actively discussed at business unit meetings. Employees have a clear understanding of how to identify and escalate potential cybersecurity issues.
	Intermediate	Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable. The risk culture requires formal consideration of cyber risks in all business decisions. Cyber risk reporting is presented and discussed at the independent risk management meetings.
	Advanced	Management ensures continuous improvement of cyber risk cultural awareness.
	Innovative	The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon.

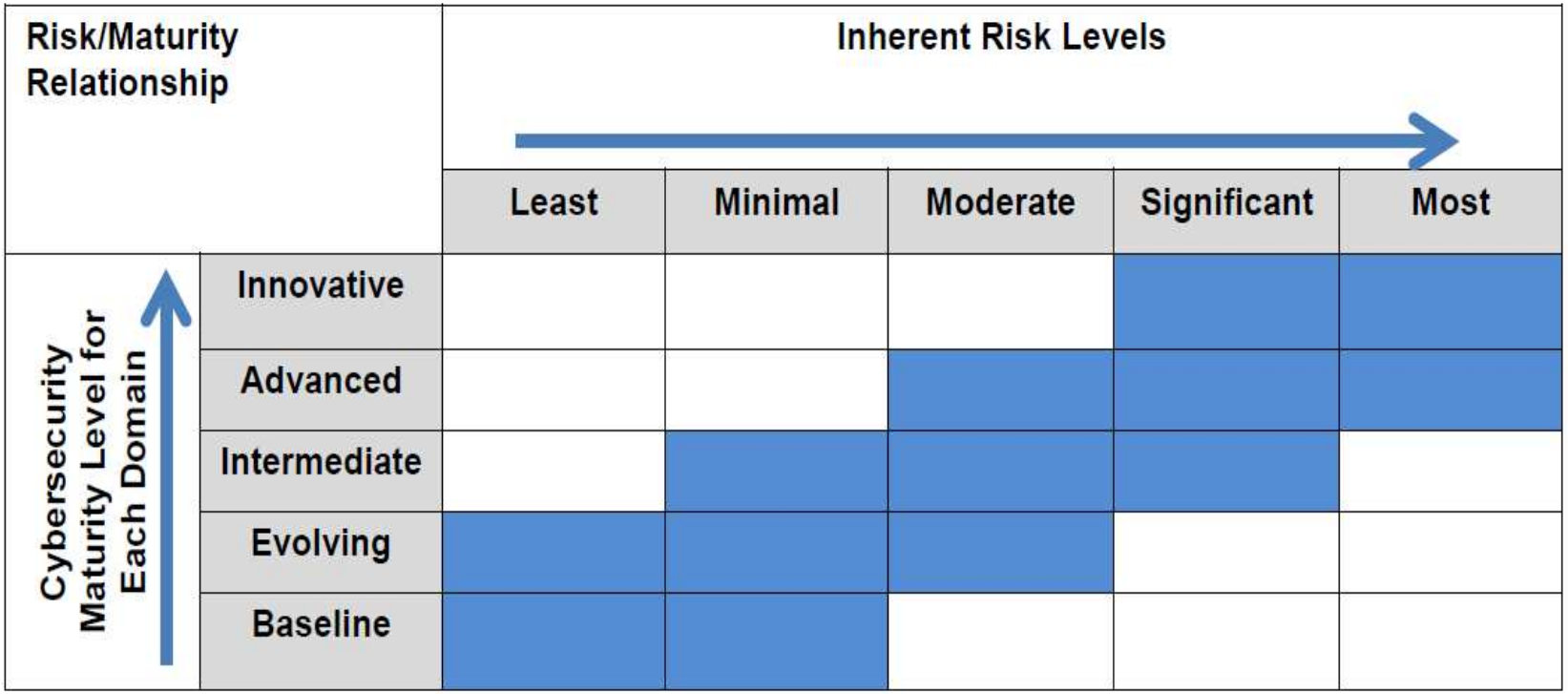
babc

FFIEC Cybersecurity Assessment Tool: Cybersecurity Maturity

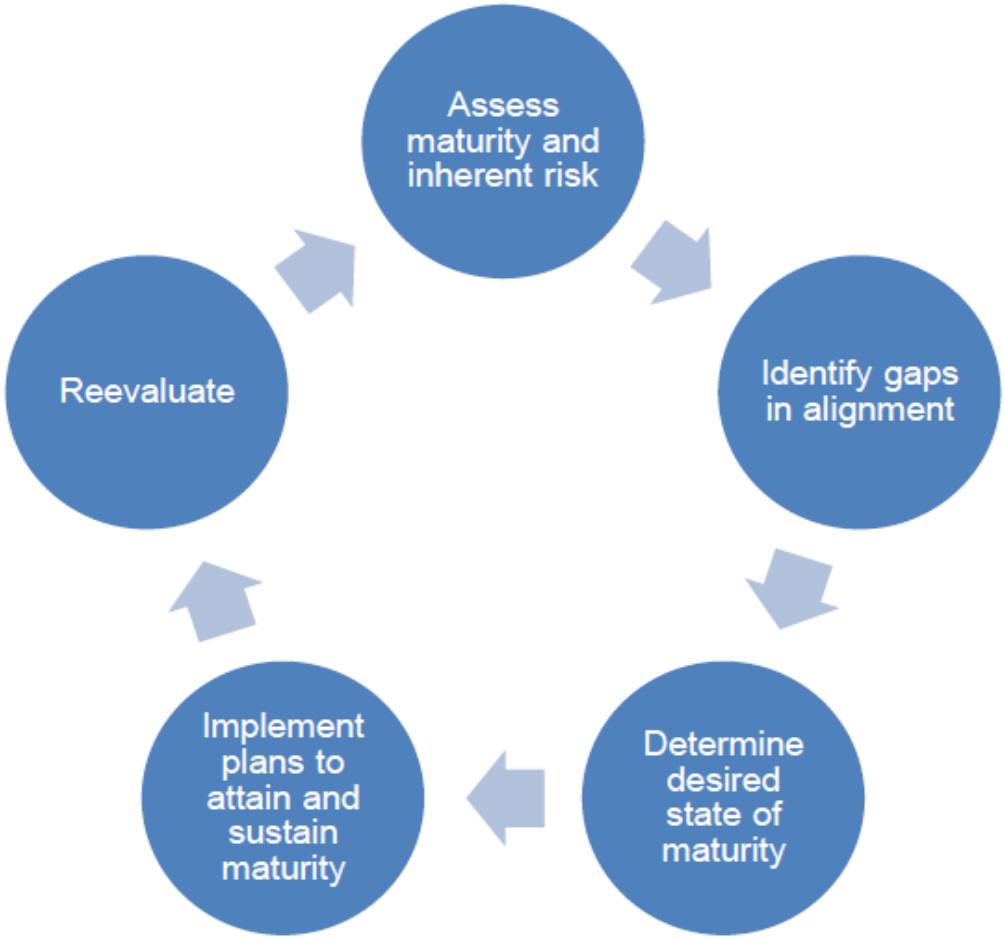


- **Baseline – Characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed the evaluated guidance.**

FFIEC Cybersecurity Assessment Tool: Mapping Inherent Risk Against Cybersecurity Maturity



FFIEC Cybersecurity Assessment Tool: Evolving Process



FFIEC Cybersecurity Assessment Tool:
Board (and Management) Oversight

- **Risk Management Oversight**
  - What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities?
  - How is accountability determined for managing cyber risks across our enterprise? Does this include management's accountability for business decisions that may introduce new cyber risks?
  - What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

- **Cyber Security Controls**
  - What is our process for classifying data and determining appropriate controls based on risk?
  - What is our process for ensuring that risks identified through our detective controls are remediated?

- **Cyber Incident Management and Resilience**
  - In the event of a cyber attack, how will we respond internally and with customers, third parties, regulators, and law enforcement?
  - How are cyber incident scenarios incorporated in our business continuity and disaster recovery plans? Have these plans been tested?

Source: Federal Financial Institutions Examination Council (FFIEC)

"Recurring Issues" in Healthcare Enforcement

1. Risk Analysis
2. Vendor (Business Associate) Agreements
3. Failure to Manage Identified Risk, e.g. Encrypt
4. Lack of Transmission Security
5. Lack of Appropriate Auditing
6. No Patching of Software
7. Insider Threat
8. Improper Disposal
9. Insufficient Data Backup and Contingency Planning

- Many have RA+, NY/Columbia $4.8M, St. Elizabeth: document sharing application to store PHI without analyzing risk $250K
- Almost 1000 cloud providers/hospital
- Concentra $1.7M – stolen unencrypted laptop
- Anchorage Community Mental Health – Malware from unpatched vulnerabilities $150K
- Cornell Prescription Rx $125K

Resolution Agreements often involve allegations of widespread noncompliance, lack of any risk analysis.

Source: US HHS Office for Civil Rights (OCR), 9/2015

Questions?

Paige M. Boshell
205.521.8639
pboshell@babc.com
www.babc.com/paige-m-boshell

Amy S. Leopard
615.252.2309
aleopard@babc.com
www.babc.com/amy-s-leopard